

Forum:[Hack Forums](#)

Thread: [\[TuT\] Extracting Files From Wireshark - Kali Linux](#)

SIM-5561 - August 17, 2013, 5:22 am

Intro + About Me

As I'm now a 'l33t' member, I'm going to pay the board back by doing some HQ tutorials. There is no bullshit here, just information. I'm a fully qualified forensic analyst with 5 years experience in the IT industry. I'm no skid. This is legit stuff. What you do with this information is up to you, but by reading this post, you acknowledge that I have no responsibility for your actions. With that being said, let's begin:

Extracting Files From Wireshark Tutorial by Puzzle9

We're going to be working with Wireshark. For those who don't know, Wireshark is a swiss army knife when it comes to computing. Wireshark can capture every single packet sent from a source computer to a destination computer/server. In one word, I would describe it as: ultimate.

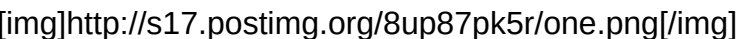
But can anyone use Wireshark? My answer is No. But wait...you can learn Wireshark! There is hope. Wireshark is a pro tool because it is essentially showing you exactly what is going on with your network. So it's your duty to learn networking inside out. You can still use Wireshark without being a network expert, but honestly, your skills will be more or less laughable. So get learning!

So, what are we going to do for this tutorial? Well, we're going to look at a trace file and carve out a document that was sent via instant message. Huh? We're what!?! Wireshark lets you capture packets and save them as a 'pcap'. So I've got a 'pcap' file ready and I'm going to open it and take screenshots along the way so you can keep up visually.

Wireshark comes installed on Kali Linux, so just open the terminal, type wireshark followed by enter, otherwise you can do the following to open Wireshark within Kali:

Quote:Information Gathering > Traffic Analysis > Wireshark

In Wireshark, go to File, Open. Browse to your pcap file and it will look like this:

Spoiler [\(Click to View\)](#)[img]http://s17.postimg.org/8up87pk5r/one.png[/img]

This is just a personal thing, but I always go to the top menu of Wireshark and hit Statistics > Protocol Hierarchy. This lets us see all the different protocols we're dealing with. In my case, I'm dealing with IPv4, SSL, UDP, but mainly TCP. What do we know about TCP? Well TCP isn't a best effort protocol. TCP wants to send exactly the right packets down the line. So already I have a sneaky suspicion that there MAY have been a file sent/downloaded because there is so much TCP packets in this trace.

So you can close the statistics and now take a look at the packets themselves. So now, I'm going to look at the bytes displayed in the 3rd frame. Why? Well I'm looking for a conversation, so the plaintext conversation will be displayed in bytes down at the bottom (I hope).

And without much effort, it looks like I found the conversation under a packet using the SSL protocol (see pic below). If I right click the packet and click follow tcp stream, I can view what looks

like a complete mess of a conversation.

Packet:

Spoiler ([Click to View](#))[img]http://s9.postimg.org/y6rim2x3z/convo.png[/img]

Stream:

Spoiler ([Click to View](#))[img]http://s21.postimg.org/3mvmytmqv/stream.png[/img]

If you look closely, you'll make out something that says: recipe.docx (or whatever the document is called). So now, I know that my target was sending a document file to someone. I need to carve that document out of the packet. So, how do I do it?

Clear the filter, because it doesn't look like the file is in this packet, since it's too small. Click:

Quote:Analyze - Expert Info > details (tab)

From here you can see what ports were used for various connections. I spotted a TCP sequence where a connection was established to a server port on packet 109. You will probably find the same although it will be a different packet number. You have to search for it. I can't 'teach' that part. See screenshot below:

Spoiler ([Click to View](#))[img]http://s24.postimg.org/44pvbqbud/expert_Info.png[/img]

This looks much more like it. recipe.docx is mentioned here and now, all I need to do is save the TCP stream onto my desktop in Kali. So, click the drop down menu and select the one with the most bytes. In my case, the TCP stream was 12264 bytes which is around 12kb. Click save as and save to desktop. My filename is: puzzle9.docx. We can now close Wireshark.

Now, I downloaded open office, because Kali cannot open docx files without a 3rd party piece of software, I installed open office. You can install open office by opening the terminal and run the following command:

Quote:apt-get install openoffice.org

Hit Y followed by enter and wait for it to install.

Now, try opening your document. There's a pretty damn good chance it won't work. Any ideas why? Well you've just copied a conversation from a packet in the TCP protocol. That means your file has got junk before the header, so basically, Microsoft Office or OpenOffice doesn't know what the hell it is and will throw up an error message. Try it. Once you've installed Open Office, try open the word file. It will look like this:

Spoiler ([Click to View](#))[img]http://s22.postimg.org/3nwukfo9t/trying_To_Open_Docx.png[/img]
We need to delve into hex.

To install a hex editor on Kali, do the following:

- 1) Open terminal
- 2) Run this command: Quote:leafpad /etc/apt/sources.list
- 3) Add the new source of Kali repository below, then save and exit.

Quote:deb <http://mirror.nus.edu.sg/kali/kali> kali main

- 4) Run update of apt and install the hexedit package.

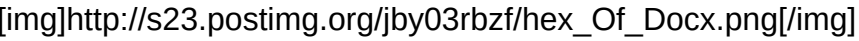
Quote:apt-get update && apt-get install hexedit

Note: I find hex editors to be rubbish on Linux. I ended up using Windows/Mac hex editors to finish

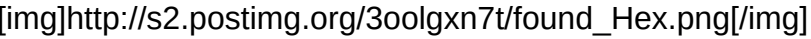
this tut.

Excellent. So now that's installed, from the terminal, change the cwd (current working directory) to your desktop, or wherever you saved the docx file from Wireshark. Type in: hexedit

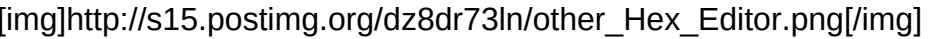
The hex editor will ask what file you want to open. Type in the filename, so in my case, it's puzzle9.docx

Spoiler ([Click to View](#))

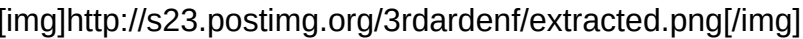
Quote: Search for the following hex: 50 4B 03 04

Spoiler ([Click to View](#))

When you find it, delete everything before it (see screenshot below this paragraph). Once you've done this, close your hex editor and save the changes.

Spoiler ([Click to View](#))

Open the file and you have now successfully extracted a word document sent during an SSL encrypted chat / file transfer.

Spoiler ([Click to View](#))

Competition + Free eBook

First one to decrypt the message in my .docx file will win a steam key for Ostfront: 41-45. Please comment and/or give rep if you enjoyed this tutorial and I will do more.

I am giving away a 100% FREE eWhoring eBook, written by ME. If you wish to have it, please PM me and I will send it to you as quick as I can.

Cicada - August 17, 2013, 10:25 am

Awesome tutorial! was hoping to see something like this pop up
thanks :D

reama - August 17, 2013, 11:20 am

Nice tut sometimes wireshark can be a real pain. thx!
-rec

cpl220101 - August 17, 2013, 9:23 pm

How'd you know to search for "50 4B 03 04"? I saw the OTF2 header, just like a MZ or JFIF header, but how'd you know the exact set of hex characters?

fissionxedge1110 - August 17, 2013, 9:33 pm

Vouch for puzzle!

Damn good tutorial. I've never done this before, and I've always wanted to. I think I'll write a tool to automate the process a little bit.

SIM-5561 - August 17, 2013, 11:38 pm

(Aug 17, 2013 09:23 PM)cpl220101 Wrote: [CITE](#) How'd you know to search for "50 4B 03 04"? I saw the OTF2 header, just like a MZ or JFIF header, but how'd you know the exact set of hex characters?

Because every file has a magic number. So I knew docx's, it was just a matter of finding it.

Paradoxmoney - August 18, 2013, 4:56 am

nice tutorial mate , hq post for share

GoneByTheWind - *August 18, 2013, 7:05 am*

Good tutorial! Just started learning forensics and I'm sure these tutorials you're doing willl help alot :)
Thanks for that.